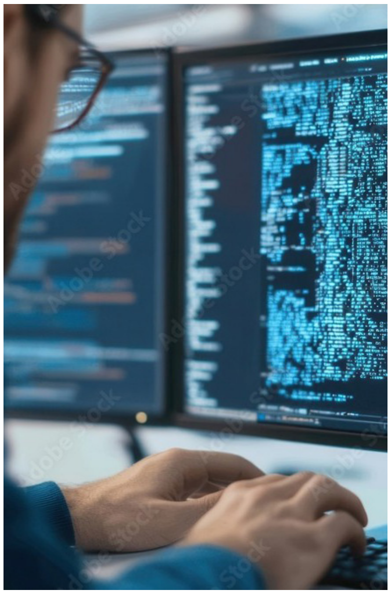
AVALON

Types of Penetration Testing



Penetration testing **validates the efficiency of your currently deployed security resources** and determines how well **employees are following existing security policies.**

Typically implemented on an annual basis, penetration testing validates the efficiency of your currently deployed security resources and determines how well employees are following existing security policies. If we detect any weaknesses, we will work with you to develop solutions and strengthen security controls within your company.

INTERNAL PENETRATION TESTING

A simulated cyberattack conducted from within an organization's network to identify and exploit security weaknesses that a malicious insider or compromised internal device could leverage.

Focus areas: Lateral movement, privilege escalation, data exfiltration

Value: Tests internal defenses and response capabilities, assuming perimeter defenses have failed

EXTERNAL PENETRATION TESTING

A simulated cyberattack performed from outside an organization's network to identify and exploit vulnerabilities in internet-facing systems such as web servers, firewalls, and email services.

Focus areas: Firewalls, VPNs, web servers, email gateways

Value: Identifies vulnerabilities that could be exploited from the internet

WEB APPLICATION PENETRATION TESTING

A security assessment that simulates attacks on a custom or third-party web application to identify vulnerabilities such as SQL injection, cross-site scripting (XSS), and authentication flaws.

Focus areas: OWASP Top 10 vulnerabilities, authentication and session management, input validation

Value: Ensures applications are secure against common and advanced attack vectors

WIRELESS PENETRATION TESTING

The process of assessing the security of wireless networks by stimulating attacks to identify vulnerabilities in protocols, configurations, and connected services.

Focus areas: Rogue access points, encryption protocols, signal leakage

Value: Protects against unauthorized access and data interception via wireless networks

SOCIAL ENGINEERING TESTING

This evaluates an organization's susceptibility to manipulation by simulating attacks that exploit human behavior to gain unauthorized access to systems or sensitive information.

Focus areas: Phishing campaigns, pretexting, tailgating

Value: Identifies weaknesses in employee awareness and training

PHYSICAL PENETRATION TESTING

This involves simulating real-world attacks to assess the effectiveness of physical security controls in preventing unauthorized access to buildings, assets, or sensitive areas.

Focus areas: Facility access controls, surveillance systems, badge cloning

Value: Validates physical security controls and response procedures

CLOUD PENETRATION TESTING

The process of simulating attacks on cloud-based environments to identify and remediate security vulnerabilities in configurations, applications, and infrastructure.

Focus areas: IAM policies, misconfigurations, API security

Value: Ensures cloud environments are securely configured and monitored

Turning the Tables on

CYBER BREACHES

How Incident Response Tabletop Exercises Prepare Your Organization For Cyber Threats

AVALON

Don't miss out on more free content from Team Avalon!

Join the Avalon mailing list to receive useful case studies, industry insights, handy tips, and more delivered straight to your inbox.

Sign up to receive exclusive content!

AVALON

QUESTIONS?

For more information on any of our services, please contact:

Rebecca Rudell, Marketing Manager
rebecca.rudell@teamavalon.com